"Countering CCP Drones Act" – Frequently Asked Questions

What is the "Countering CCP Drones Act," and what does it do?

The "Countering CCP Drones Act" is a bill (HR 2684) which would require the Federal Communications Commission (FCC) to add DJI to its "Covered List." If DJI is added to this list, the FCC could no longer approve new equipment authorizations for DJI products in the United States. The Agency could also create a process to revoke existing authorizations. This means that no new DJI products could be approved in the U.S. going forward, and the DJI drones currently approved for U.S. use may be grounded in the future.

What does the "Countering CCP Drones Act" mean for the drones I already have?

The "Countering CCP Drones Act" may not have an immediate impact on your current drone fleet. However, the FCC has the power to create a process to revoke the equipment authorizations for your existing drone models in the future, which would mean the federal government could decide at any point that you are no longer allowed to fly the DJI drones you have already purchased, no matter if you are flying them for business, public safety or even recreationally.

What will the "Countering CCP Drones Act" mean for future models of DJI drones?

The "Countering CCP Drones Act" would prohibit the FCC from authorizing or even reviewing equipment authorizations for new DJI products. This means that new DJI models would not be able to be sold or used in the United States going forward, cutting you off from the latest cutting-edge technology from DJI.

What does the "Countering CCP Drones Act" mean for the drone industry as a whole?

The "Countering CCP Drones Act" would have a massive impact for the drone industry writ large and even the broader U.S. economy. According to a 2023 economic impact analysis by John Dunham & Associates, removing DJI and its products from the market would result in the closure of 67% of American small drone businesses and the loss of more than 450,000 U.S. jobs. In addition, cutting the leading manufacturer out of the drone market would lead to rising costs and product shortages for all users. It also takes a life-saving tool out of the hands of first responders, putting lives on the line.

What data security safeguards does DJI have in place?

First, DJI drones feature a default "opt-in" approach to sharing photos, videos or flight logs – if users do not want to share that data with DJI, they don't have to. If a user does wish to store their flight log data, it is kept in U.S.-based servers such as AWS.

Additionally, DJI drones feature a "Local Data Mode" that keeps all data private by turning off the connection between the drone and the internet, and keeps data stored on the drone/SD card, the remote controller or the app. When Local Data Mode is on, the app will close all data services and will not send any network requests.

Users also can bypass the DJI flight app by using third-party software developed and owned by American companies. These third-party options can be downloaded onto the iPad or Android device and used as a separate app, allowing the user to avoid interacting with DJI software at all.

Has DJI's data security been confirmed by outside organizations?

Yes. Several government agencies and independent private sector firms have analyzed DJI products and issued reports attesting to their security. For example:

- San Francisco cybersecurity firm Kivu Consulting conducted a first-of-its-kind detailed examination of DJI drones, mobile apps, and servers, as well as the data streams they transmit and receive. Kivu purchased DJI drones off the shelf, downloaded DJI software from the Internet, then scrutinized every bit of data they exchanged over the Internet to determine whether customer data was in fact protected. The ensuing report concluded that DJI did not access photos, videos, or flight logs generated by the drones unless drone operators voluntarily chose to share them.
- A risk assessment conducted by Booz Allen Hamilton tested the data security of certain DJI drones and found no evidence that the data, or information collected by these drones was transmitted to DJI, China or any other unauthorized party.
- FTI Consulting found when Local Data Mode is enabled, "no data that was generated by the application was sent externally to infrastructure operated by any third party, including DJI." In its cybersecurity assessment, it also noted "a number of instances where DJI employed security best practices." The report also noted that when users opted to share their data with DJI, there was no data transmission to Chinese servers. All data went to servers in the U.S., or western Europe.
- The U.S. Department of the Interior (DOI), which has used drones for monitoring wildfires, conducting geological surveys, and inspecting volcanic activity, conducted a flight test and technical evaluation of its DJI drones. After a careful evaluation, DOI concluded that DJI drones were the best suited for accomplishing their missions while at the same time protecting the data they generate.
- The Idaho National Laboratory, which conducted a cybersecurity test and evaluation of two DJI drones on behalf of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, found that "there are no major areas of concern related to data leakage."
- The U.S. Department of Commerce validated DJI's Core Crypto Engine, confirming it meets NIST standard FIPS 140-2, for cybersecurity relating to government procurement.